Jefferson. University Hospitals

URGENT — Please Open Immediately.

Family of

ID TheftSmart™

JAKE SCHIED
Membership Number:

Member Services: 1-866-599-4455
9:00 a.m. to 6:00 p.m. (Eastern Time), Monday through Friday
If you have questions or feel an identity theft issue may be present, please call ID TheftSmart member services.

July 22, 2010

Dear Family of

As the president of Thomas Jefferson University Hospitals (TJUH), I need to make you aware of a computer theft which occurred last month in one of our facilities. Regretfully, this incident may have a personal impact on the individual named above.

On June 14, 2010, an employee reported to TJUH security personnel that his password-protected personal laptop computer was stolen from an office in our hospital. Because information was being temporarily stored on the computer, we want to let you know what happened, what we are doing to prevent such an incident from happening again and provide you with information on the identity protection resources we are making available—at our expense—to help protect the patient's information moving forward.

The computer contained medical data from individuals who received inpatient care at the hospital during a six-month period in 2008. The information was being utilized as part of a quality review process we use to improve patient care. Though the computer was password-protected, it was not hospital-issued and the data was not encrypted.

Information on the computer included: name, birth date, gender, ethnicity, diagnosis, social security number, insurance information, hospital account number and other internal and administrative coding. To date, there has been no indication of inappropriate use of any information stored on the stolen computer.

TJUH has extensive internal policies reflecting our commitment to the appropriate use of personal health information and employees receive training on these policies annually. The storage of patient data on an employee's unencrypted computer—even while on TJUH premises—is a breach of hospital policy.

Subsequent to notifying local police, the hospital privately retained resources through Kroll Inc. to assist with our internal investigation and to provide you with special personal assistance. Key personnel have been interviewed, specific policy violations have been addressed, and we have taken appropriate actions with the employees involved.

Additionally, the hospital is reviewing protocols and will be reinforcing these protocols through employee education conducted across the enterprise.

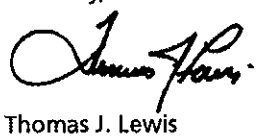
TJUH is committed to protecting both your health and your health information. Through our engagement with Kroll, we are making substantial identity theft safe guards available to you at our expense.

- **Enhanced Identity Theft Consultation and Restoration.** Licensed Investigators, who truly understand the problems surrounding identity theft, are available to listen, to answer your questions, and to offer their expertise regarding any concerns you may have. Should your name and credit be affected by this incident, your investigator will help restore your identity to pre-theft status.

If you have questions, please call **1-866-599-4455**, 9:00 a.m. to 6:00 p.m. (Eastern Time), Monday – Friday. In addition, please review all credit card bills, invoices and bank statements you may receive, and immediately report any suspicious activity to Kroll at the above number.

On behalf of everyone at Jefferson Hospitals, please accept our apologies and know that we are committed to providing assistance, should you require it, and to safeguarding the privacy of your personal health information.

Sincerely,



Thomas J. Lewis
President and Chief Executive Officer

U.S. State Notification Requirements

For residents of *Hawaii, Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, Vermont, Virginia, West Virginia,* and *Wyoming*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax
P.O. Box 740241
Atlanta, Georgia 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022
1-800-888-4213
www.transunion.com

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of *Maryland* and *North Carolina*:
You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take to avoid identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft/

For residents of *Massachusetts* and *West Virginia*:
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit.

To place a security freeze on your credit report, you need to send a request to a consumer reporting agency by certified mail, overnight mail, or regular stamped mail. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion (FVAD)
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

214-0709 ICR

If you feel you have an identity theft issue, call us today using the toll-free telephone number listed in the accompanying letter.

Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.

Help is only a phone call away.

Legal Remedy. Any Stolen Identity Event where the victim is unwilling to prosecute the person who caused the victim to suffer the fraud or its consequences.

Dishonest Acts. Any dishonest, criminal, malicious, or fraudulent acts, if the Member(s) that suffered the fraud personally participated in, directed, or had knowledge of such acts.

Financial Loss. Membership Services do not cover any financial losses attributed to the Stolen Identity Event, including but not limited to, money stolen from a wallet, unauthorized purchases of retail goods, or services online, by phone, mail, or direct.

Pre-existing Stolen Identity Event Limitations. If either the victim had knowledge of, or reasonably should have had knowledge of, a pre-existing stolen identity event (not this one) based on information provided to them prior to enrollment in the program, such an event or the consequences caused by it are not covered.

Business. A covered stolen identity event does not include the theft or unauthorized or illegal use of their business name, DBA, or any other method of identifying their business activity.

Minors. Minors are fundamentally excluded given that (a) credit reporting agencies do not knowingly maintain credit files on minor children, and (b) minor children are unable to execute the Limited Power of Attorney (LPoA) required for certain processes as described herein. However, Kroll agrees to try to resolve identity theft issues for participant-minors through the processes listed in the master agreement, with additional reasonable efforts to address the challenges of working with minors, and within the solutions available through existing legislation and established industry and organizational procedures.

IDTheftSmart

Helping

Millions of People

Safeguard Their Identities